UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

EVALUACIÓN DE LA EFICIENCIA DE TÉCNICAS DE CRIPTOGRAFÍA EN LA PROTECCIÓN DE DATOS CONFIDENCIALES

AUTOR:

CHRISTIAN PATRICIO ILBAY TAPIA

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR
2025

Autor:

Christian Patricio Ilbay Tapia
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
cilbay@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero de Sistemas.
Magister en Sistemas de Calidad y Productividad.
mquiroz@ups.edu.ec

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS
2025 © Universidad Politécnica Salesiana.
CUENCA – ECUADOR – SUDAMÉRICA
CHRISTIAN PATRICIO ILBAY TAPIA
Evaluación de la eficiencia de técnicas de criptografía en la protección de datos confidenciales

DEDICATORIA

El presente trabajo le dedico principalmente a Dios, quien me ha dado la fuerza para culminar uno de mis anhelos más deseados. Sin Su guía, nada de esto habría sido posible.

También dedico este trabajo con todo mi amor y gratitud a mis padres, quienes han sido mi mayor ejemplo de esfuerzo, perseverancia y fe.

AGRADECIMIENTO

Agradezco a Dios por bendecir mi vida, guiarme a lo largo de mi vida personal y profesional y por ser la fortaleza en aquellos momentos de dificultad y debilidad.

Gracias a mis padres Norma y Marcelo por sus enseñanzas y por siempre confiar en mí y alentarme a crecer cada día más y no rendirme hasta conseguir mis objetivos.

Finalmente, a los docentes de la Maestría en Seguridad de la Información de la Universidad Politécnica Salesiana por haber compartido sus conocimientos a lo largo del programa, de manera especial a mi tutor quien me ha brindado su apoyo profesional en este trabajo.

Tabla de Contenidos

Evaluación de la eficiencia de técnicas de criptografía en la protección de datos confidenciales

Autor:

Christian Patricio Ilbay Tapia

RESUMEN

La criptografía es un enfoque que ayuda a asegurar la transmisión de datos, esta técnica oculta los datos y los cambia a un formato ilegible, en caso que una entidad no autorizada obtiene los datos es imposible hacer legibles los datos. Es necesario la seguridad y la privacidad de la información, que permita al dueño confiar en los entornos o sistemas, que permita al propietario cifrar o descifrar su información, sin tener desventajas o complejidad o pérdida de tiempo, sin ser ineficiente para el procesamiento. El objetivo general de esta investigación es evaluar la eficiencia de técnicas de criptografía para determinar los mejores algoritmos aplicando el método AHP-Topsis. En la metodología se utiliza la investigación exploratoria para identificar algoritmos criptográficos en los artículos científicos, se utiliza la revisión sistemática, el enfoque cualitativo, el enfoque cuantitativo. Entre los resultados, la matriz de decisiones presentó como mejor alternativa el algoritmo criptográfico RSA (Rivest-Shamir-Adleman) con 5.17 de peso. La segunda alternativa es el algoritmo MD5 (Message-Digest Algorithm 5) con 5.05 de peso. La tercera alternativa es SHA (Secure Hash Algorithm) con 5.03 de peso. El resultado final presenta que los algoritmos criptográficos ya clasificados con TOPSIS confirma que RSA es la primera y mejor alternativa. Además, RSA es utilizado en 13 de 33 artículos seleccionados en la revisión sistemática. En esta era que la seguridad de la información es importante para conservar la Confidencialidad, Integridad y Disponibilidad de los recursos digitales; es básico adoptar modelos que ayuden en la preservación de la Seguridad y Privacidad.

Palabras clave: Técnicas de criptografía, Algoritmos criptográficos, AHP, Topsis.

ABSTRACT

Cryptography is an approach that helps secure the transmission of data, this technique hides the data and changes it to an unreadable format, in case an unauthorized entity obtains the data it is impossible to make the data readable. There is a need for information security and privacy, which allows the owner to trust the environments or systems, which allows the owner to encrypt or decrypt their information, without having disadvantages or complexity or loss of time, without being inefficient for processing. The general objective of this research is to evaluate the efficiency of cryptography techniques to determine the best algorithms by applying the AHP-Topsis method. In the methodology, exploratory research is used to identify cryptographic algorithms in scientific articles, systematic review, qualitative approach, quantitative approach are used. Among the results, the decision matrix presented the RSA (Rivest-Shamir-Adleman) cryptographic algorithm with 5.17 weight as the best alternative. The second alternative is the MD5 (Message-Digest Algorithm 5) algorithm with 5.05 weight. The third alternative is SHA (Secure Hash Algorithm) with 5.03 in weight. The final result presents that the cryptographic algorithms already classified with TOPSIS confirms that RSA is the first and best alternative. In addition, RSA is used in 13 of 33 articles selected in the systematic review. In this era that information security is important to preserve the Confidentiality, Integrity and Availability of digital resources; it is essential to adopt models that help in the preservation of Security and Privacy.

Keywords: Cryptography Techniques, Cryptographic Algorithms, AHP, Topsis.

1. Introducción

En la actualidad, la criptografía es importante porque las tecnologías como IoT, Blockchain y Cloud Computing utilizan las técnicas para minimizar o mitigar los intentos de violación a los datos en cualquier entorno y permitir el acceso a la información confidencial; la criptografía es preservar la privacidad de la información a través de operaciones matemáticas para que el destinatario o recurso permitido pueda leer el dato que está cifrado; la criptografía es una prioridad para todo usuario a nivel general (Yadav & Kumar, 2023).

El problema que se aborda en esta investigación es la selección de una de las técnicas de cifrado como DES, AES, SHA, MD5, RSA, DHELLMAN, ECC, ElGamal, IMM, LBC y Blow Fish, determinando la más recomendable para su utilización. Aunque, existen más técnicas solo se evalúan las nombradas.

Por otra parte, algunas razones de este estudio son porque el uso no adecuado de un cifrado puede conllevar consecuencias, como mala operación del funcionamiento en dispositivos, accesos no autorizados a datos privados, o seleccionar técnicas no conocidas al cifrar los datos de cada usuario; existe la posibilidad que todos los algoritmos no sean la opción correcta para todos los casos, sea por capacidades del entorno o hardware como el caso de dispositivos portátiles.

El presente trabajo tiene como objetivo el evaluar la eficiencia de técnicas de criptografía para determinar los mejores algoritmos aplicando el método Topsis. Para desarrollar el objetivo se realiza lo siguiente: analizar las técnicas de criptografía en artículos científicos a través de una revisión literaria, luego se realiza una evaluación teórica de la eficiencia de los algoritmos criptográficos mediante el método AHP-Topsis, finalmente se analiza las comparaciones para recomendar el algoritmo mejor puntuado.

2. Estudios previos

La investigación de Zubair y Ahmed realiza una exploración de varios algoritmos criptográficos, hace un análisis comparativo entre cantidad del bloque, tamaño de la clave y ciclos para medir el rendimiento; investigaron las técnicas simétricas y asimétricas, se enfocaron en la banca electrónica, comercio electrónico y salud; enfatizan la importancia del avance en criptografía que garantice la seguridad (Zubair & Ahmed, 2024). Los investigadores examinaron las técnicas como BLOWFISH, DES, EIGAMAL, RSA, SHA y TEA; compararon el tamaño del bloque, tamaño de clave, tiempo de cifrado, tiempo de descifrado, consumo de energía y velocidad; de acuerdo a las pruebas, el algoritmo RSA es el mejor puntuado (Surla & Lakshmi, 2023). Basri y otros, analizaron el algoritmo DES y la esteganografía que se utiliza para computación en la nube al almacenar archivos y mensajes, la seguridad y confidencialidad mejoran con la ronda de 16 bloques porque la versión anterior funcionaba a 8 bloques que la hacía menos segura (Basri et al., 2021). En este trabajo, se analizan los algoritmos Beaufort y Hill entre valores de clave, texto modificado, cantidad de bits cambiados y efecto; luego de la comparación realizan un cifrado de doble capa por medio de estos dos cifrados para generar un tercer algoritmo de cifrado; este tercer algoritmo ofrece mejores resultados (Fadlan et al., 2022). Este trabajo explora métodos que preservan la integridad de la clave de cifrado, y busca fortalecer protocolos de seguridad de datos con el algoritmo AES, mejora el cifrado pesado y contribuye en las prácticas criptográficas (Rani et al., 2023). Los autores propusieron un cifrado de clave pública y tiene búsqueda eficiente, utiliza el algoritmo Diffie-Hellman para mostrar la resistencia a los ataques; el análisis teórico muestra un esquema que logra una seguridad sólida y gran eficiencia (Wu et al., 2021). El documento presenta un análisis sobre el cifrado, descifrado, claves públicas RSA y utilización en el ámbito militar, empresarial y seguridad de la información; describe el uso de algoritmo RSA en la vida privada, e implementan una solución para realizar el cifrado/descifrado con RSA; el programa es una nueva versión basado en RSA (Zhou & Tang, 2021).

En este estudio se implementó la curva elíptica (ECC) y ElGamal para almacenar y obtener información desde bases de datos, evitar que terceros conozcan los elementos dentro del cifrado, y aumentar la seguridad de los datos entre dos partes (Mousay et al., 2023).

Los autores propusieron la implementación de normas de seguridad en una empresa de servicio de transporte naviero y proponen algunos aspectos para la seguridad de información en una investigación cualitativa, además de identificar sus obstáculos en el momento de implantar el sistema de gestión (Preciado & Quiroz, 2022). La propuesta propone la seguridad de la información mediante protocolos y redundancia de red y, corrección de posibles vulnerabilidades, y configuración de una red eficiente para garantizar la confidencialidad, integridad y disponibilidad (Cisneros et al., 2023). Los autores propusieron una metodología básica en las pequeñas y medianas empresas financieras para clasificar los activos de información y analizar los riesgos relacionados a seguridad de la información; la propuesta se basa en norma de seguridad 27005 (Hugo & Quiroz, 2024). Otro tipo de seguridad basado en norma 27001 fue propuesta para la implementación en la seguridad de la información y gestión de los procesos empresariales (Álava et al., 2023). El estudio se enfocó en implementar un plan ante incidentes sobre la seguridad de datos sensibles en un hospital público; identificaron los activos críticos y evaluaron los riesgos, actividades de detección temprana e identificación de posibles anomalías (Buenaño et al., 2024). Con el trabajo de investigación se identificó las vulnerabilidades en seguridad de la información dentro de una empresa de transporte de carga, con ello se presentó un plan de acción basado en la norma 27001; para evitar el acceso de intrusos, posible pérdida y exposición de datos, daños por virus, y alteraciones de datos (Choez et al., 2023). Este último estudio analiza la combinación de seguridad con otras tecnologías IoT y Big Data en la gestión de datos viales, proponen un modelo teórico basado en estas tecnologías para mejorar la integridad de los datos y monitoreo en tiempo real (Quiroz-Martinez et al., 2024).

3. Materiales y Metodología

Para el desarrollo del estudio se aplicó el método empírico-analítico basado en evidencias del cual se dividió en 3 fases, se utilizó el enfoque cuantitativo en las evaluaciones, se utilizó el enfoque cualitativo en los hallazgos, la técnica de la deducción.

En la primera fase, se analizaron las técnicas de criptografía hallados en artículos científicos, se adoptó de (Rey et al., 2021) las actividades de Revisión Sistemática de la Literatura que asisten en la identificación y categorización de artículos sobre Técnicas de Criptografía; la exploración se realiza en tres bibliotecas digitales Association for Computing Machinery, IEEE y Springer, que consta de tres etapas: Planificación, Realización e Informe.

La etapa Planificación es la revisión del estado del arte de cada artículo con respecto a técnicas de criptografía; se propusieron las preguntas de investigación (PI): PI1: ¿Cuáles son los algoritmos criptográficos encontrados?, PI2: ¿Cuáles son los dominios en que se utilizan los algoritmos?, PI3: ¿Cuáles son los alcances de los artículos?, PI4: ¿Cuáles son los datos de ejecuciones en las comparativas?, PI5: ¿Cuáles son los parámetros utilizados en las comparaciones?

Estas preguntas de investigación se obtuvieron desde los artículos científicos, son preguntas o afirmaciones más comunes halladas durante la lectura de los artículos, como los nombres de los algoritmos, áreas de utilización, comparativas o parámetros.

La etapa Realización: Se identificaron los artículos científicos, la búsqueda se enfoca en tres bibliotecas; aquí se realizan cuatro tareas: 1) Exploración en las Bibliotecas, se busca en los títulos y/o palabras con la cadena de búsqueda: “cryptography”. 2) Discriminación con criterios de inclusión-exclusión, el filtro es sobre el título y/o resumen del artículo científico. Criterios de Inclusión: artículos desde año 2020, artículos en inglés, artículos con modelos criptográficos. Criterios de Exclusión:

artículos sólo resumen, tesis, monografías. 3) Búsqueda Bola de Nieve, para mejorar las consultas, utilizar una sola interacción hacia atrás y hacia adelante que ratifica el artículo que puede ser pasado por alto en la primera búsqueda. 4) Evaluación de la metodología, se explora para confirmar los artículos principales, se realiza otra exploración en las diferentes bibliotecas.

La etapa Informe: Esta fase se realizó en la fase resultados del artículo, con los datos extraídos en las fases de Planificación y Realización; se presenta el análisis cuantitativo que responde las preguntas de investigación.

En la segunda fase, se realizó una evaluación teórica de la eficiencia de los algoritmos criptográficos; se obtuvieron las características de los algoritmos hallados en las investigaciones científicas y se tomaron los datos de las comparaciones existentes en los artículos. Se utiliza el método AHP-Topsis (Cherier et al., 2021), de acuerdo a los artículos científicos la metodología AHP-TOPSIS es considerada como una base de decisión de apoyo. El AHP ayuda determinar la importancia relativa de varios criterios en un problema de decisión; mediante AHP esta importancia relativa se establece mediante los pasos:

1) Determinar una matriz de comparación por pares

$$\left[a_{ij}\right]_{n\,x\,n} \tag{1}$$

Aquí $\boldsymbol{a_{ij}}$ es la importancia relativa del criterio desde ***i*** hasta ***j***.

Con una valoración subjetiva de cada par de criterios fundada en la escala de 9 puntos de Saaty.

$$\begin{bmatrix} a_{11} & a_{12} \dots & a_{1n} \\ a_{21} & a_{22} \dots & a_{2n} \\ \vdots & & \vdots \\ a_{n1} & a_{n2} \dots & a_{nn} \end{bmatrix} \tag{2}$$

Aquí, ***n*** es el número de criterios, llamados atributos de decisión.

2) Generar una matriz de decisión se normaliza con la fórmula.

$$m_{ij} = \frac{C_{ij}}{\sum_{j=i}^{n} C_{ij}} \quad (3)$$

m es una matriz de comparación cuya diagonal es 1 y el número (*mij*) para la comparación por pares indica la preferencia entre los elementos *i* sobre *j*.

3) Calcular las ponderaciones de los criterios y verificar la coherencia, luego generar una matriz de decisión normalizada ponderada.

$$W = [w_i]_{n\,x\,1} \quad (4)$$

i = 1, 2, 3 … n, *j* = 1, 2, 3 … n

$$w_i = \sum_{j=1} \frac{m_{ij}}{n} \quad (5)$$

Una vez formada la matriz de comparación, el vector de pesos *W* se puede determinar mediante (4)

4) Generar una matriz de decisión normalizada para las comparaciones entre criterios, los datos se normalizan como sigue:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum x_{ij}^2}} \quad (6)$$

Aquí, $\boldsymbol{x_{ij}}$ es el valor de la ***i***-ésima alternativa con respecto al ***j***-ésimo criterio para ***i*** = 1,…, m; ***j*** = 1,…, n.

5) La matriz normalizada ponderada $\boldsymbol{v_{ij}}$ se establece multiplicando cada columna de la matriz $\boldsymbol{r_{ij}}$ por el peso $\boldsymbol{w_j}$, alcanzado por AHP.
6) Las soluciones ideales, es decir, la mejor y las peor ideal negativa, se descubren mediante la fórmula mostrada a continuación, donde J = (j = 1, 2… n)/j está enlazada con los atributos beneficiosos y J' = (j = 1, 2, …, n)/j está enlazada con los atributos no beneficiosos.

   El máximo valor de beneficio y el mínimo valor de los atributos de costo son para la solución ideal positiva (A+):

$$A^{+} = \{(\sum_i^{max} v_{ij}|j\epsilon J), (\sum_i^{min} v_{ij}|j\epsilon J^i)| = 1,2..m\} = \{v_1^{+}, v_2^{+}, v_3^{+}, \dots v_n^{+}\} \quad (7)$$

Mientras que el mínimo valor de beneficio y el máximo valor de costo son para la ideal solución negativa (A-):

$$A^{-} = \{(\sum_i^{max} v_{ij}|j\epsilon J), (\sum_i^{min} v_{ij}|j\epsilon J^i)| = 1,2..m\} = \{v_1^{-}, v_2^{-}, v_3^{-}, \dots v_n^{-}\} \quad (8)$$

Aquí, *i* se asocia con criterios de beneficio y *J* se asocia con criterios no beneficiosos.

7) El trayecto por cada alternativa a la ideal solución se obtiene mediante la fórmula (***i*** = 1, 2, … m):

$$s_i^{+} = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^{+})^2} \quad (9)$$

La distancia desde la solución ideal negativa es obtenida:

$$s_i^{-} = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^{-})^2} \quad (10)$$

8) La cercanía relativa a la solución ideal se obtiene por la ecuación:

$$C_i^{*} = (S_i^{-})/(S_i^{+} + S_i^{-}) \quad (11)$$

9) Se clasifican las alternativas de acuerdo a los valores de cercanía relativa Ci* en orden descendente. Es decir, un valor de cercanía relativa alto es la mejor alternativa.

En la tercera fase, se analizaron las comparaciones y se recomienda el algoritmo mejor puntuado; se analizó las medidas y comparaciones de los modelos con diferentes parámetros, analizar la posible correlación entre los modelos, confirmar los cifrados más fuertes, describir las posibles limitaciones, describir la matriz comparativa, matriz de evaluación, matriz de decisión normalizada, el resultados de evaluación de los algoritmos.

4. Resultados y discusión

La revisión sistemática dio como resultado 31 artículos de los cuales se extrajo las características: lista de algoritmos criptográficos, nombre de áreas-dominios, objetivos de los artículos, datos considerados en las ejecuciones y parámetros revisados en los artículos. En la figura 1 se presentan los artículos que inician en ámbito de criptografía, y luego los clasifica en algoritmos, aplicaciones, conceptos relacionados, técnicas relacionadas, evaluaciones y protocolos. Luego se sub clasifica los algoritmos en simétricos, asimétricos y hash, y estos últimos se describen en los nombres de las técnicas de cifrado. Los algoritmos fueron evaluados en tiempos, eficiencia, consumo de energía, técnica de avalancha e implementaciones. En contextos de utilización como IoT, nube, aplicaciones electrónicas, chip, sector bancario.

Figura 1.

Mapa conceptual de artículos seleccionados

Nota: Distribución de los documentos.

Estos 31 artículos ayudaron a responder y analizar las preguntas de investigación. La tabla 1 presenta los artículos obtenidos de la revisión sistemática.

Tabla 1.

Documentos analizados.

Artículo	Cantidad
(Khan et al., 2021), (Mallouli & Hellal, 2021), (Salman, 2021), (Rahman & Hossain, 2021), (Akmuratovich & Salimboyevich, 2021), (Fotovvat et al., 2021), (Wang, 2021), (Shin & Kwon, 2021), (V. Kumar, 2021), (Sharma & Pokharana, 2021), (Tajammul et al., 2021), (Pavani & Sriramya, 2021), (Raya & Mariyappn, 2021), (Mandal et al., 2021), (Chandra et al., 2021), (Semwal & Sharma, 2021), (Suta Atmaja & Arya Astawa, 2021),	22

(Liestyowati, 2021), (Martino & Cilardo, 2021), (Davenport & Shetty, 2021), (Zheng et al., 2021), (Celik et al., 2021)	
(Shaikh & Nenova, 2022), (Bhardwaj et al., 2022), (Sivajyothi & Devi, 2022), (S. Kumar & Deora, 2022), (Halak et al., 2022), (Lino & Cecilio, 2022)	6
(Yadav & Kumar, 2023), (Kaur et al., 2023), (Oladipupo et al., 2023)	3
Total	31

Nota: Lista de artículos seleccionados de la revisión sistemática.

De la revisión sistemática se contestaron las preguntas de investigación descritas en la metodología.

PI1: ¿Cuáles son los algoritmos criptográficos encontrados?: Entre los 31 artículos se hallaron los siguientes algoritmos criptográficos: DES en 12% (8 ocasiones), AES en 20% (13 ocasiones), SHA en 9% (6 ocasiones), MD5 en 1% (1 ocasión), RSA en 20% (13 ocasiones), DHELLMAN en 1% (1 ocasión), ECC en 20% (13 ocasiones), ElGamal en 9% (en 5 ocasiones), IMM en 1% (1 ocasión), LBC en 1% (1 ocasión), Blow Fish en 6% (4 ocasiones). La palabra “ocasiones” significa que un algoritmo fue nombrado/utilizado en los diferentes artículos. Aquí, los algoritmos AES (Estándar de cifrado evolucionado), ECC (Cifrado de curva elíptica) y RSA (Rivest, Shamir y Adleman) son los más utilizados en 20% cada uno, es decir los tres suman 60% a nivel de los artículos utilizados.

PI2: ¿Cuáles son los dominios en que se utilizan los algoritmos?: Entre los 31 artículos se hallaron las áreas que se nombran como: IoT en 31% (10 ocasiones), Blockchain en 6% (2 ocasiones), Archivos en 38% (12 ocasiones), Nube en 16% (5 ocasiones), Salud en 6% (2 ocasiones), Video en 3% (1 ocasión). Las pruebas e implementaciones realizadas por los artículos científicos fueron sobre cualquier tipo de archivo en 38%; luego le sigue las propuestas en Internet de las Cosas en 31%. Se deduce que en la mayoría de los casos los algoritmos criptográficos se utilizan para asegurar la información en la obtención, almacenamiento y transmisión a través de archivos y/o dispositivos. Además, se resalta que la tecnología Blockchain utiliza el algoritmo SHA (Algoritmo hash seguro) versión SHA256 para cifrar todos los bloques de almacenamiento, los certificados de

autenticidad. Por otra parte, la Nube también utiliza algoritmos para garantizar a sus clientes: la integridad y confidencialidad de la información.

PI3: ¿Cuáles son los alcances de los artículos?: Entre los 31 artículos se hallaron los objetivos generales como: Versiones en 32% (12 ocasiones), Comparaciones en 46% (17 ocasiones), y Solo Ejecución en 22% (8 ocasiones). El 46% de los artículos realizaron comparaciones entre los algoritmos criptográficos, además las comparaciones se realizaron entre diferentes versiones y versiones originales. Otros artículos solo confirmaron el cifrado por ejecución.

PI4: ¿Cuáles son los datos de ejecuciones en las comparativas?: Entre los 31 artículos, estos analizaron los datos como: Tiempo en Segundos por 36% (19 ocasiones), Bytes en 47% (25 ocasiones) y Hardware en 17% (9 ocasiones). Aquí, solo 19 artículos compararon en Segundos/Bytes sus ejercicios, aunque algunos miden en kilobytes o megabytes, se tomó como medida básica el Byte; además 6 artículos sólo realizaron comparaciones de almacenamiento en Bytes. Los artículos que ejecutaron con parámetro Hardware son operaciones sobre área Internet de las Cosas.

PI5: ¿Cuáles son los parámetros utilizados en las comparaciones?: Entre los 31 artículos, estos hallaron los parámetros como: Almacenamiento con 16% (12 ocasiones), Cifrado en 37% (27 ocasiones), Descifrado en 36% (26 ocasiones), y Correlación en 11% (8 ocasiones). Los artículos realizaron trabajos de cifrado y descifrado en conjunto en 73%, es decir que los algoritmos fueron comprobados por los autores para utilizarlos en sus propuestas. La correlación significa que los artículos realizaron comparaciones porcentuales entre los algoritmos utilizados. El almacenamiento se utiliza en seguridad de archivos locales o en la nube.

Para la evaluación teórica mediante AHP-Topsis, se utilizó como Criterios las características halladas en los artículos científicos de la revisión sistemática, y son los siguientes: Dominios (IoT, Blockchain, Archivos, Nube, Video), Alcances (Versiones, Comparaciones, Solo Ejecución), Datos de ejecuciones (Segundos,

Bytes, Hardware) y Parámetros (Almacenamiento, Cifrado, Descifrado, Correlación). Estos criterios se denominan desde CR01 hasta CR15.

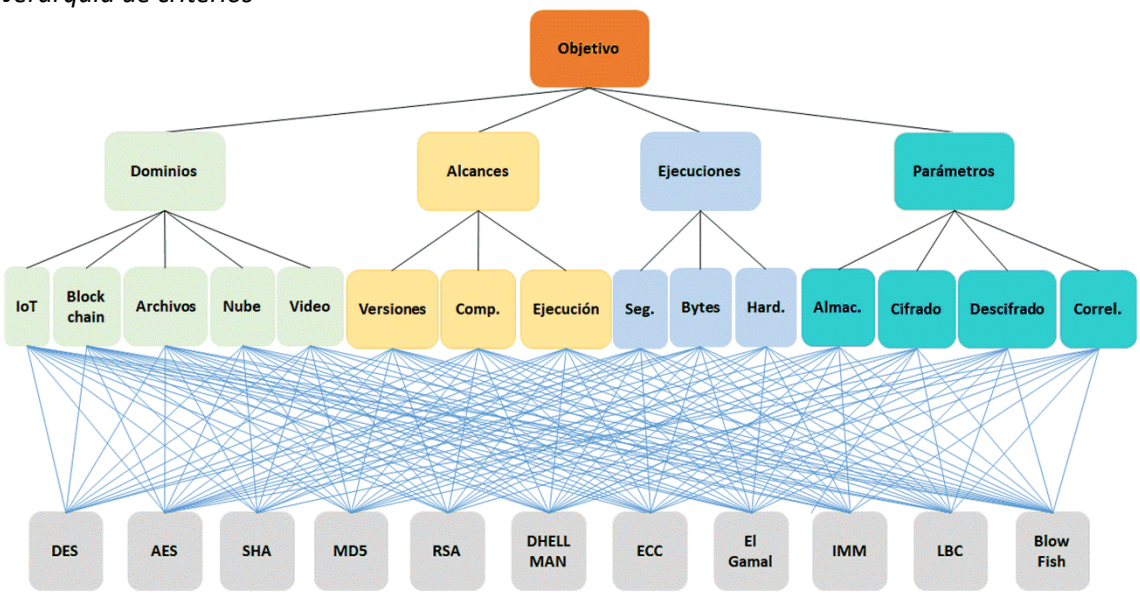
Y como alternativas se utilizaron los algoritmos criptográficos encontrados en los artículos científicos con los algoritmos utilizados en las técnicas como son: DES, AES, SHA, MD5, RSA, DHELLMAN, ECC, ElGamal, IMM, LBC y Blow Fish.

AHP se utilizó como un instrumento para toma de decisiones para evaluar la eficiencia de los algoritmos criptográficos, AHP simplifica este problema por medio de la descomposición de los criterios en una estructura jerárquica multinivel; aquí se utilizaron los objetivos Dominios, Alcances, Datos de ejecuciones y Parámetros; y subjetivos: Correlación (CR01), Descifrado (CR02), Cifrado (CR03), Almacenamiento (CR04), Hardware (CR05), Bytes (CR06), Segundos (CR07), Solo Ejecución (CR08), Comparaciones (CR09), Versiones (CR10), Video (CR11), Nube (CR12), Archivos (CR13), Blockchain (CR14), IoT (CR15). Ver figura 2.

Esto es para clasificar las salidas factibles que son los algoritmos criptográficos.

Figura 2.

Jerarquía de criterios



Nota: Objetivos y criterios.

TOPSIS se utilizó como proceso de toma de decisiones multicriterio; aquí el mejor algoritmo criptográfico está cerca de la resolución ideal positiva y lejos de la

resolución ideal negativa; es decir, se escoge un algoritmo que maximice los criterios de seguridad y minimice los criterios de riesgos (Patil & Singh, 2023).

Se evalúa una matriz de decisión matriz [*m* x *n*] que contiene *m* alternativas, se evalúan en términos de *n* criterios. Los principales pasos básicos son: a) Construcción de la matriz ponderada, b) Determinación de soluciones, c) Cálculo de las medidas de separación. d) Calculo de la solución ideal.

Una matriz de comparación por pares matriz [15x15] (Tabla 2) se establece de acuerdo a las preferencias para tomar las decisiones, mediante la escala de 9 puntos de Saaty. Los 15 criterios se generan en la matriz para comparar el grado Relativo entre 2 criterios. La normalización en la matriz ayuda en el cálculo de los pesos o ponderaciones de los criterios (CR01 hasta CR15).

Tabla 2.

Matriz de criterios de comparación por parejas

Código	Criterios	CR01	CR02	CR03	CR04	CR05	CR06	CR07	CR08	CR09	CR10	CR11	CR12	CR13	CR14	CR15	Sum	Weights
CR01	Correlación	1	2	5	3	7	9	4	5	1	5	8	2	6	4	3	65.00	0.1156
CR02	Descifrado	1/2	1	2	5	9	3	5	8	5	2	4	6	4	2	6	62.50	0.1112
CR03	Cifrado	1/5	1/2	1	4	7	4	6	9	6	7	5	7	5	2	3	66.70	0.1186
CR04	Almacenamiento	1/6	1/4	1/5	1	3	1	2	3	2	8	7	8	1	4	2	42.62	0.0758
CR05	Hardware	1/7	1/9	1/4	1/2	1	9	1	5	8	8	4	5	8	4	8	62.00	0.1103
CR06	Bytes	1/9	1/3	1/4	1/6	1/6	1	5	1	7	8	2	3	1	1	8	38.03	0.0676
CR07	Segundos	1/4	1/5	1/6	1/7	1	1/5	1	9	6	7	5	1	7	7	4	48.96	0.0871
CR08	Ejecución	1/5	1/8	1/9	1/2	1/5	1	1/9	1	1	2	1	7	3	6	7	30.25	0.0538
CR09	Comparaciones	1	1/5	1/6	1/8	1/8	1/7	1/6	1	1	5	4	6	2	8	3	31.93	0.0568
CR10	Versiones	1/5	1/2	1/3	1/9	1/8	1/8	1/7	1/2	1/5	1	7	9	8	3	7	37.24	0.0662
CR11	Video	1/8	1/4	1	1/2	1/4	1/2	1/5	1	1/4	1/7	1	2	7	5	2	21.22	0.0377
CR12	Nube	1/2	1/6	1/7	1/7	1/5	1/3	1	1/7	1/6	1/9	1/2	1	8	2	3	17.41	0.0310
CR13	Archivos	1/3	1/2	1/5	1/5	1/5	1	1/3	1/3	1/2	1/2	1/2	1/2	8	4	7	24.10	0.0429
CR14	Blockchain	1/4	1/2	1/2	1/4	1/4	1	1/7	1/6	1/8	1/3	1/5	1/2	1/4	1	4	9.47	0.0168
CR15	IoT	1/3	1/3	1/3	1/7	1/8	1/8	1/4	1/7	1/3	1/7	1/2	1/3	1/2	1/4	1	4.85	0.0086
																	562.26	1.0000

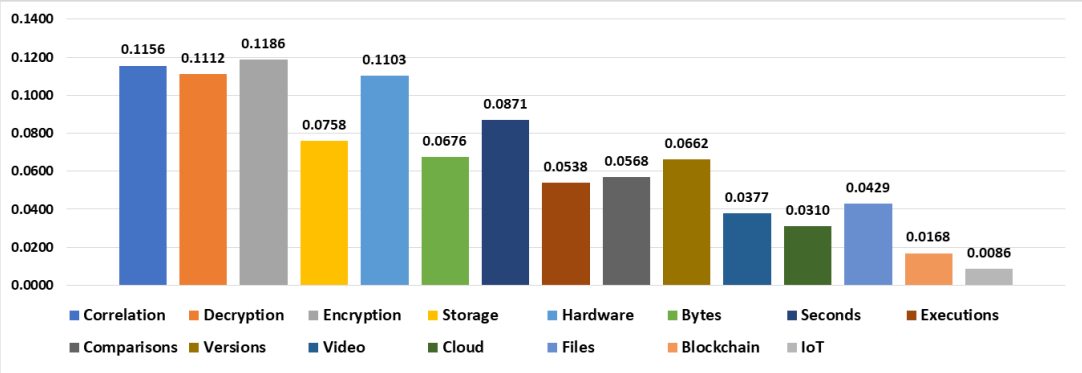
Nota: Los criterios de selección de la jerarquía.

Este peso revela el grado entregado a cada criterio, aquí la tabla 3 muestra la matriz normalizada y sus pesos de los criterios.

La matriz de criterios muestra que el mayor peso 0.1186 está en el criterio “Cifrado”, luego el peso 0.1156 en el criterio “Correlación” y luego el peso 1112 en el criterio “Descifrado”. La última columna de la tabla 3 se procesa para establecer los pesos relativos de los criterios mediante el marco de cálculo de valores propios de AHP. La figura 3 también muestra los pesos referentes-relativos de los criterios en forma de columnas y diferenciadas por colores.

Figura 3.

Criterios



Nota: Representación de los pesos.

Se establece una matriz normalizada ponderada *matriz* [*m* x *n*] es decir *matriz* [*11 x 15*] y procesar esta matriz mediante TOPSIS para obtener el ranking de los algoritmos criptográficos considerados. Se utiliza la matriz de decisión (tabla 2) y las ponderaciones de los criterios, para implementar una matriz normalizada ponderada (Tabla 3). En la tabla 3, por cada Técnica Criptográfica se da una calificación en los criterios, entre mayor número es mejor puntaje. Este último puntaje se multiplica por el peso de cada Criterio (CR01 hasta CR15). La multiplicación genera un puntaje por cada criterio, es decir existen 15 puntajes de criterios por cada técnica. Luego se suman los puntajes de cada criterio y se obtiene un total de la técnica. La matriz de decisiones obtiene como mejor alternativa el algoritmo criptográfico RSA que tiene 5.17 peso. La segunda alternativa es el algoritmo MD5 que tiene 5.0537 peso. La tercera alternativa es SHA.

Tabla 3.

Matriz de decisiones ponderada-normalizada

	CR01	CR02	CR03	CR04	CR05	CR06	CR07	CR08	CR09	CR10	CR11	CR12	CR13	CR14	CR15 S	Total
DES	1.0405	0.1112	0.8304	0.3032	0.1103	0.2029	0.5225	0.3766	0.2839	0.4636	0.0377	0.0619	0.0857	0.0505	0.0689	4.5498
AES	0.3468	0.2223	0.2373	0.3032	0.8822	0.2705	0.1742	0.4304	0.3975	0.1987	0.3396	0.1548	0.2143	0.0674	0.0345	3.5016
IMM	1.0405	0.1112	0.5931	0.3790	0.6617	0.3382	0.2612	0.1076	0.2271	0.0662	0.0377	0.1238	0.0429	0.0337	0.0862	3.5587
MD5	0.5780	0.5558	0.3559	0.6822	0.2206	0.4058	0.5225	0.5380	0.3975	0.3974	0.1509	0.0619	0.0857	0.1516	0.0603	5.0537
RSA	0.8092	1.1116	0.8304	0.0758	0.3308	0.1353	0.6966	0.5380	0.1703	0.1325	0.1509	0.1548	0.0857	0.1347	0.0345	5.1706
DHELLMAN	0.2312	0.6670	0.2373	0.1516	0.8822	0.1353	0.7837	0.3228	0.3975	0.4636	0.3774	0.0310	0.3000	0.0505	0.0431	4.3021
ECC	0.1156	0.1112	0.5931	0.0758	1.1028	0.3382	0.1742	0.3228	0.3407	0.3311	0.0377	0.3096	0.1286	0.0674	0.0172	3.0734
ElGamal	0.8092	0.1112	0.5931	0.0758	0.4411	0.6763	0.0871	0.4842	0.0568	0.3974	0.2264	0.1857	0.3000	0.0337	0.0862	4.2334
SHA	0.5780	0.6670	0.7118	0.0758	0.3308	0.4734	0.6095	0.2690	0.4543	0.2649	0.3396	0.0619	0.3429	0.0674	0.0086	5.0344
LBC	0.1156	0.2223	0.4745	0.4548	0.9925	0.6763	0.6095	0.3766	0.2839	0.2649	0.3019	0.1857	0.2143	0.1684	0.0776	4.5367
BlowFish	0.1156	0.3335	0.5931	0.2274	0.6617	0.4734	0.2612	0.3228	0.5678	0.6623	0.0755	0.1238	0.2572	0.0842	0.0689	4.2771
A+	1.0405	1.1116	0.8304	0.6822	1.1028	0.6763	0.7837	0.5380	0.5678	0.6623	0.3774	0.3096	0.3429	0.1684	0.0862	
A-	0.1156	0.1112	0.2373	0.0758	0.1103	0.1353	0.0871	0.1076	0.0568	0.0662	0.0377	0.0310	0.0429	0.0337	0.0086	

Nota: Algoritmos de cifrado y los criterios de selección.

Una vez obtenidos los pesos de cada criterio mediante el método AHP, se realizó el procedimiento TOPSIS que utiliza la matriz de decisión normalizada ponderada Tabla 3. TOPSIS es un método para la toma de decisiones multicriterio para seleccionar el mejor algoritmo criptográfico que debe estar lo más cerca de la solución ideal positiva y lo más lejos de la solución ideal negativa. Es decir, se debe seleccionar el mejor algoritmo criptográfico que maximice los criterios de beneficio y minimice los criterios de costo.

Se calcularon las distancias de separación, mediante la Distancia Euclidiana de *n* dimensiones, luego se calculó la cercanía relativa a la ideal solución, que están reflejadas como *Si+* y *Si-*; luego se clasificaron las alternativas (algoritmos criptográficos) en orden descendente de acuerdo a la cercanía relativa *Pi*.

El resultado final se presenta los algoritmos criptográficos ya clasificados en la Tabla 4. TOPSIS confirma que el algoritmo RSA es la primera y mejor alternativa.

Tabla 4.

Ranking de alternativas

Alternativas	Si+	Si-	Ci	Rank
DES	1.6808	1.3197	0.4398	6
AES	1.6317	1.0558	0.3929	11
IMM	1.6265	1.2219	0.4290	8
MD5	1.3952	1.2294	0.4684	5
RSA	1.3789	1.5803	0.5340	1
DHELLMAN	1.4273	1.3829	0.4921	2
ECC	1.7748	1.2016	0.4037	10
ElGamal	1.6714	1.1803	0.4139	9
SHA	1.3352	1.2612	0.4857	3
LBC	1.4728	1.3659	0.4812	4
BlowFish	1.5554	1.1716	0.4296	7

Nota: Algoritmos de cifrado obtenidos en la revisión sistemática.

Análisis: Con la premisa de verificar la coherencia, los resultados de la evaluación de algoritmos criptográficos se calcularon mediante el modelo AHP-TOPSIS, además, se obtuvo las distancias geométricas de los algoritmos ideales positivos y negativos. El algoritmo criptográfico RSA es más influyente, seguida por DHELLMAN y luego por SHA.

RSA es utilizado en 13 de 33 artículos seleccionados en la revisión sistemática, que son: (Lino & Cecilio, 2022), (V. Kumar, 2021), (Yadav & Kumar, 2023), (Davenport & Shetty, 2021), (Tajammul et al., 2021), (Suta Atmaja & Arya Astawa, 2021), (Pavani & Sriramya, 2021), (Liestyowati, 2021), (Raya & Mariyappn, 2021), (Akmuratovich & Salimboyevich, 2021), (Mallouli & Hellal, 2021), (Semwal & Sharma, 2021), (S. Kumar & Deora, 2022). Por otra parte, el artículo (Lino & Cecilio, 2022) realizó pruebas con siete algoritmos: DES, AES, SHA, MD5, RSA, DHELLMAN y ECC. El artículo (S. Kumar & Deora, 2022) realizó pruebas con seis algoritmos: DES, AES, SHA, RSA, ElGamal y Blow Fish. Ver tabla 5.

El *Cifrado* es el peso más alto entre los criterios principales (11.86%), seguido por la *Correlación* (11.56%), Descifrado (11.12%). Por otro lado, de acuerdo a la revisión sistemática, los algoritmos AES, RSA y ECC en 20% cada uno. Aunque, AHP-TOPSIS confirma que RSA es el algoritmo mejor recomendado, seguido por DHELMAN y SHA.

Este estudio comprende una representación de los criterios en la selección de un algoritmo criptográfico, se determinaron quince criterios principales para analizar la selección. Un problema común en seleccionar un algoritmo, involucra la evaluación de datos cuantitativos y cualitativos. La comparación por pares en la información de AHP ayudó a entender la importancia de los criterios de selección. En el caso aplicado, se distingue que los criterios de Parámetros obtuvieron los pesos máximos, el sub-criterio Cifrado tiene 0.1186; lo cual se debe a la importancia fundamental de ocultar los datos. Luego le sigue el criterio de Ejecuciones, Alcances y Dominios. En criterio Ejecuciones, el sub-criterio Hardware tuvo 0.1103 como mayor ponderación. Esto indica que el criterio Parámetros tiene prioridad sobre los criterios de Ejecuciones, y confirma que los parámetros de los algoritmos criptográficos son más importantes que los tipos de Ejecuciones.

Tabla 5.

Evaluación final de alternativas

Artículo	DES	AES	SHA	MD5	RSA	DHELLMAN	ECC	ElGamal	IMM	LBC	Blow Fish
(Lino & Cecilio, 2022)	1	1	1	1	1	1	1				
(V. Kumar, 2021)					1		1				
(Salman, 2021)							1				
(Yadav & Kumar, 2023)		1			1						
(Sivajyothi & Devi, 2022)		1					1				
(Sharma & Pokharana, 2021)		1					1				
(Davenport & Shetty, 2021)					1		1			1	
(Tajammul et al., 2021)	1	1			1						1
(Fotovvat et al., 2021)		1									
(Suta Atmaja & Arya Astawa, 2021)					1						
(Pavani & Sriramya, 2021)					1						
(Rahman & Hossain, 2021)							1		1		
(Khan et al., 2021)							1				
(Celik et al., 2021)		1									
(Liestyowati, 2021)					1						
(Wang, 2021)			1								
(Raya & Mariyappn, 2021)	1				1		1	1			
(Akmuratovich & Salimboyevich, 2021)	1				1			1			
(Oladipupo et al., 2023)							1				
(Halak et al., 2022)		1									
(Martino & Cilardo, 2021)			1								
(Shin & Kwon, 2021)		1	1				1				
(Kaur et al., 2023)			1								
(Mallouli & Hellal, 2021)					1		1	1			
(Mandal et al., 2021)	1	1									1
(Chandra et al., 2021)	1	1						1			
(Semwal & Sharma, 2021)	1	1			1						1
(Shaikh & Nenova, 2022)							1				
(S. Kumar & Deora, 2022)	1	1	1		1			1			1
Totales	8	13	6	1	13	1	13	5	1	1	4
Porcentajes	12%	20%	9%	1%	20%	1%	20%	9%	1%	1%	6%

Nota: Lista de artículos obtenidos en la revisión sistemática.

6. Conclusiones

Este artículo presentado se basó en el marco AHP-TOPSIS para seleccionar entre 11 algoritmos criptográficos de acuerdo a un conjunto de 15 criterios. Se utilizó el método AHP para identificar las puntuaciones de cada criterio, y el método TOPSIS utilizó esas puntuaciones computadas de AHP para clasificar los algoritmos criptográficos.

El marco AHP-TOPSIS es una herramienta muy útil que ayudó en la selección de algoritmos para garantizar el mejor cifrado o encriptación de información; el marco utilizado puede ser aplicado a otras alternativas como tecnologías o software que brinden seguridad a la información con similares características.

Es posible adicionar otros criterios o sub-criterios al modelo de jerarquía para obtener otros casos de estudio. El trabajo desarrollado utiliza la metodología AHP y TOPSIS para priorizar los once algoritmos y seleccionar el mejor algoritmo basado en un entorno de toma de decisiones con múltiples criterios. En este artículo el método AHP y el método TOPSIS coinciden en la selección del algoritmo criptográfico RSA como el mejor para el cifrado de información.

Este estudio empírico demuestra que aplicar o basarse en AHP-TOPSIS es factible y más sencillo para obtener el mejor algoritmo criptográfico como es RSA. En esta era que la seguridad de la información es importante para conservar la Confidencialidad, Integridad y Disponibilidad de los recursos digitales; mientras que Internet abre más amenazas, vulnerabilidades y riesgos, es básico adoptar modelos que ayuden en la preservación de la Seguridad y Privacidad.

Referencias

Akmuratovich, S. M., & Salimboyevich, O. I. (2021). A Creation Cryptographic Protocol for the Division of Mutual Authentication and Session Key. *ICISCT 2021*, 1–6. https://doi.org/10.1109/ICISCT52966.2021.9670057

Álava, M., Choez, H., & Quiroz, M. (2023). Diseño de un SGSI basado en el estándar ISO 27001 para la empresa Invimedic S.A. *Univerdidad Politecnica Salesiana*. http://dspace.ups.edu.ec/handle/123456789/26680

Basri, M., Mawengkang, H., & Zamzami, E. M. (2021). Cloud Computing Security Model with Combination of Data Encryption Standard Algorithm (DES) and Least Significant Bit (LSB). *Journal of Physics: Conference Series*, *970*(1). https://doi.org/10.1088/1742-6596/970/1/012027

Bhardwaj, C., Garg, H., & Shekhar, S. (2022). An Approach for Securing QR code using Cryptography and Visual Cryptography. *Proceedings of International Conference on Computational Intelligence and Sustainable Engineering Solution, CISES 2022*, 284–288. https://doi.org/10.1109/CISES54857.2022.9844332

Buenaño, J., Cusme, C., & Quiroz, M. (2024). Plan de respuesta a incidentes de seguridad cibernética para hospital público. *Univerdidad Politecnica Salesiana*. http://dspace.ups.edu.ec/handle/123456789/29344

Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. (2021). Program Analysis of Commodity IoT Applications for Security and Privacy. *ACM Computing Surveys*, *52*(4), 1–30. https://doi.org/10.1145/3333501

Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2021). A comparative survey of symmetric and asymmetric key cryptography. *Nternational Conference on Electronics, Communication and Computational Engineering, ICECCE*, 83–93. https://doi.org/10.1109/ICECCE.2014.7086640

Cherier, M. A., Bennekrouf, M., & Meliani, S. M. (2021). The Application of AHP-TOPSIS Methodology for Selection of Agriculture Farms. *International Colloquium*, 0–4. https://doi.org/10.1109/LOGISTIQUA49782.2020.9353915

Choez, J., Quispe, A., & Ríos, M. (2023). Análisis de vulnerabilidades del sistema de información del área de logística de la empresa Transcarga S.A. *Univerdidad Politecnica Salesiana*. http://dspace.ups.edu.ec/handle/123456789/26362

Cisneros, J., Diana, L., & Quiroz, M. (2023). Propuesta de una estrategia de diseño de red de campus empresarial considerando la disponibilidad, integridad y confidencialidad de la empresa empacadora de camarones. *Univerdidad Politecnica Salesiana*, *669*. http://dspace.ups.edu.ec/handle/123456789/25188

Davenport, A., & Shetty, S. (2021). Comparative Analysis of Elliptic Curve and Lattice Based Cryptography. *Proceedings of the 2021 Annual Modeling and Simulation Conference, ANNSIM 2021*, *July 2020*, 1–9. https://doi.org/10.23919/ANNSIM52504.2021.9552144

Fadlan, M., Suprianto, Muhammad, & Amaliah, Y. (2022). Double layered text encryption using beaufort and hill cipher techniques. *International Conference on Advanced Communication Technology, ICACT Informatics and Computing*, 1–6.

https://doi.org/10.1109/ICIC50835.2020.9288538

Fotovvat, A., Rahman, G. M. E., Vedaei, S. S., & Wahid, K. A. (2021). Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes. *IEEE Internet of Things Journal*, *8*(10), 8279–8290. https://doi.org/10.1109/JIOT.2020.3044526

Halak, B., Yilmaz, Y., & Shiu, D. (2022). Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications. *IEEE Access*, *10*(July), 118522. https://doi.org/10.1109/ACCESS.2022.3219282

Hugo, C., & Quiroz, M. (2024). Propuesta de una metodología de gestión de riesgos enfocado en la seguridad de la información para las pymes financieras. *Univerdidad Politecnica Salesiana*. http://dspace.ups.edu.ec/handle/123456789/28651

Kaur, M., Alzubi, A. A., Singh, D., Kumar, V., & Lee, H. N. (2023). Lightweight Biomedical Image Encryption Approach. *IEEE Access*, *11*(July), 74048–74057. https://doi.org/10.1109/ACCESS.2023.3294570

Khan, M. N., Rao, A., & Camtepe, S. (2021). Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey. *IEEE Internet of Things Journal*, *8*(6), 4132–4156. https://doi.org/10.1109/JIOT.2020.3026493

Kumar, S., & Deora, S. S. (2022). Comparative Analysis of Security Techniques in Internet of Things. *PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing*, 407–412. https://doi.org/10.1109/PDGC56933.2022.10053313

Kumar, V. (2021). A Comparative Study of Various Lossless Compression Techniques of Steganography and Cryptography. *2021 International Conference on Computing Sciences (ICCS)*, 285–288. https://doi.org/10.1109/ICCS54944.2021.00063

Liestyowati, D. (2021). Public Key Cryptography. *Journal of Physics: Conference Series*, *1477*(5). https://doi.org/10.1088/1742-6596/1477/5/052062

Lino, I., & Cecilio, J. (2022). A Comparative Analysis of the Impact of Cryptography in IoT LoRa Applications. *IEEE International Conference on Industrial Informatics (INDIN)*, *2022-July*, 220–225. https://doi.org/10.1109/INDIN51773.2022.9976108

Mallouli, F., & Hellal, A. (2021). A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms. *EdgeCom*, 173–176. https://doi.org/10.1109/CSCloud/EdgeCom.2019.00022

Mandal, B., Chandra, S., Alam, S. S., & Patra, S. S. (2021). A comparative and analytical study on symmetric key cryptography. *International Conference on Electronics, Communication and Computational Engineering, ICECCE*, 131–136. https://doi.org/10.1109/ICECCE.2014.7086646

Martino, R., & Cilardo, A. (2021). SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey. *IEEE Access*, *8*, 28415–28436. https://doi.org/10.1109/ACCESS.2020.2972265

Mousay, F. D., Mugassabi, S. I., & Budalal, A. A. (2023). Security Measures for Ensuring Confidentiality of Information Using Encryption by Elliptic Curve with Precomputation. *2023 IEEE 11th International Conference on Systems and Control, ICSC 2023*, 938–942. https://doi.org/10.1109/ICSC58660.2023.10449816

Oladipupo, E. T., Abikoye, O. C., Imoize, A. L., Awotunde, J. B., Chang, T. Y., Lee, C. C., & Do, D. T. (2023). An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore

Wireless Sensor Networks. *IEEE Access*, *11*(January), 1306–1323. https://doi.org/10.1109/ACCESS.2022.3233632

Patil, S. S., & Singh, S. P. (2023). An AHP-TOPSIS based Decision Support Model for Selecting Biometric System. *Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023*, 272–275.

Pavani, K., & Sriramya, P. (2021). Enhancing public key cryptography using RSA, RSA-CRT and N-Prime RSA with multiple keys. *ICICV 2021*, *Icicv*, 661–667. https://doi.org/10.1109/ICICV50876.2021.9388621

Preciado, K., & Quiroz, M. (2022). Importancia de la ISO 27001 en las Pymes de Guayaquil: caso de estudio Transnave. *Univerdidad Politecnica Salesiana*, *Volumen 17*, 1–323. http://dspace.ups.edu.ec/handle/123456789/20935

Quiroz-Martinez, M., Hernandez-Romero, H., Valenzuela-Burbano, K., & Gomez-Rios, M. (2024). Prototype of a Security Model Applied to IoT with Big Data for Road Management in the City of Guayaquil. In *Lecture Notes in Networks and Systems* (pp. 564–574). https://doi.org/10.1007/978-3-031-69228-4_37

Rahman, M. S., & Hossain, M. S. (2021). Highly Area-Efficient Implementation of Modular Multiplication for Elliptic Curve Cryptography. *IEEE Region 10 Symposium, TENSYMP 2020*, *June*, 1078–1081. https://doi.org/10.1109/TENSYMP50017.2020.9230990

Rani, E., Sakthimohan, M., Amuthaguka, D., Vasanthakumar, A., Titus, J., & Premkumar, S. (2023). AES+: A Modified AES Encryption with Enhanced Key Management and Distribution. *Proceedings of the 2023 6th International Conference on Recent Trends in Advance Computing, ICRTAC 2023*, 330–335. https://doi.org/10.1109/ICRTAC59277.2023.10480804

Raya, A., & Mariyappn, K. (2021). Security and Performance of Elliptic Curve Cryptography in Resource-limited Environments: A Comparative Study. *ICITST 2021*. https://doi.org/10.23919/ICITST51030.2020.9351327

Rey, U., Carlos, J., & Bertolino, A. (2021). A Systematic Review on Cloud Testing. *ACM Computing Surveys*, *52*(5), 1–42. https://doi.org/https://doi.org/10.1145/3331447

Salman, Z. (2021). A Homomorphic Cloud Framework for Big Data Analytics Based on Elliptic Curve Cryptography. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 7–11. https://doi.org/10.1109/3ICT53449.2021.9582001

Semwal, P., & Sharma, M. K. (2021). Comparative study of different cryptographic algorithms for data security in cloud computing. *Proceedings - International Conference on Advances in Computing, Communication and Automation (Fall), ICACCA*, *January*, 1–7. https://doi.org/10.1109/ICACCAF.2017.8344738

Shaikh, J. R., & Nenova, M. (2022). Analysis of standard elliptic curves for the implementation of elliptic curve cryptography. *IEEE*, *Novem*, 1–4. https://doi.org/10.1109/COMCAS.2017.8244805

Sharma, S., & Pokharana, A. (2021). Comparative Analysis of AES-ECC and AES-ECDH Hybrid Models for a Client-Server System. *2021 2nd Global Conference for Advancement in Technology (GCAT)*, 1–7. https://doi.org/10.1109/GCAT52182.2021.9587474

Shin, S., & Kwon, T. (2021). A privacy-preserving authentication, authorization, and key

agreement scheme for wireless sensor networks in 5G-integrated internet of things. *IEEE Access*, *8*, 67555–67571. https://doi.org/10.1109/ACCESS.2020.2985719

Sivajyothi, M., & Devi, T. (2022). Analysis of Elliptic Curve Cryptography with AES for Protecting Data in Cloud. *ICIPTM 2022*, *2*(Bhosle 2013), 573–577. https://doi.org/10.1109/ICIPTM54933.2022.9753926

Surla, G., & Lakshmi, R. (2023). Performance Enhancement of State-of-the-Art Cryptography Algorithms in the Banking Sector. *Proceedings - 2023 3rd International Conference on Ubiquitous Computing and Intelligent Information Systems, ICUIS 2023*, 56–63. https://doi.org/10.1109/ICUIS60567.2023.00018

Suta Atmaja, I. M. A. D., & Arya Astawa, I. N. G. (2021). Document encryption through asymmetric RSA cryptography. *ICAST 2021*, 46–49. https://doi.org/10.1109/iCAST51016.2020.9557723

Tajammul, M., Parveen, R., & Tayubi, I. A. (2021). Comparative analysis of security algorithms used in cloud computing. *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021*, 875–880. https://doi.org/10.1109/INDIACom51348.2021.00157

Wang, B. (2021). *Research of Combining Blockchain in the Course Reform of Cryptography by Experiential Teaching*. 133–138. https://doi.org/10.1109/ICIET51873.2021.9419595

Wu, L., Chen, B., Zeadally, S., & He, D. (2021). An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage. *Soft Computing*, *22*(23), 7685–7696. https://doi.org/10.1007/s00500-018-3224-8

Yadav, V., & Kumar, M. (2023). A Hybrid Cryptography Approach Using Symmetric , Asymmetric and DNA Based Encryption. *2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 1–5. https://doi.org/10.1109/ICCT56969.2023.10076124

Zheng, G., Fang, G., Shankaran, R., & Orgun, M. A. (2021). Encryption for Implantable Medical Devices Using Modified One-Time Pads. *IEEE Access*, *3*, 825–836. https://doi.org/10.1109/ACCESS.2015.2445336

Zhou, X., & Tang, X. (2021). Research and implementation of RSA algorithm for encryption and decryption. *Proceedings of the 6th International Forum on Strategic Technology, IFOST 2011*, *2*, 1118–1121. https://doi.org/10.1109/IFOST.2011.6021216

Zubair, S., & Ahmed, H. M. A. (2024). An In-Depth Comparative Analysis of Cryptographic Techniques for Ensuring Data Privacy in E-Applications. *2024 3rd International Conference for Advancement in Technology, ICONAT 2024*, 1–8. https://doi.org/10.1109/ICONAT61936.2024.10775122